UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

UNITED STATES OF AMERICA, Plaintiff, v. Jason Gulden, Defendant.	**OBJECTION TO THE GOVERNMENT'S MOTION FOR PROTECTIVE ORDER FOR ESI** Case No.: 3:25-CR-110

The United States moves this Court for a protective order relieving it of complying the North Dakota Rules of Professional Conduct and with Rule 16 discovery obligations related to evidence it has seized but was not responsive to any warrant. The United States' motion does not identify what items it seeks protection from producing or the process by which those items were searched. The United States does not identify which devices it searched under what authority but rather asserts the conclusion that all devices except Mr. Gulden's must be protected. A search based on consent is vastly different than a search based on Federal Rule 41 which is different than a search based upon the authority of North Dakota Rule 41. The United States fails to present a record to this Court by which it can determine what, if any, good cause exists to issue a protective order. Accordingly, Mr. Gulden Objects.

BACKGROUND

Law enforcement sought and received various search warrants to search seized electronic devices. The search warrants authorized law enforcement to search the entire

device in order to identify targeted information. Law enforcement during its search of the data retained **all the data** contained on the devices searched.

Law enforcement has now split all the data it searched and retained into two categories:

- "Identified Data" – this is the data the government alleges is "within the scope of the warrants…." Doc. 130 at pg 2.

- "Remaining Data" – this is the data the government alleges "is not within the scope of the warrants…." *Id*.

Law enforcement also acquired at least one device and its data by consent[1] from the owner.

The Process

- The general process utilized by law enforcement to obtain "Identified Data" is as follows:

- **First**, law enforcement acquires a device. This is either by search warrant allowing it to seize a device containing electronically stored information and then to search the electronically stored information on the seized device, by a search

[1] Bates 1601 indicates on July 30, 2024, a DEA SA seized a cellular phone pursuant to a North Dakota search warrant. The owner of the device provided the passcode and consented to the download of the device. The device was "downloaded" on August 19, 2024, and was "processed" on September 23, 2024. All indications are that law enforcement continues to possess the device in "the vault."

warrant allowing it to seize the device then later search the device (this process is specific to Federal Rule of Criminal Procedure 41), or by consent.

- **Second**, law enforcement seized the device and all the data contained in the device.

- **Third**, at some later time, law enforcement searched all the data contained in the device.

- **Fourth**, as a result of the search in step three, law enforcement created a set of data from the seized device of which it determined it was allowed to retain possession. The possession of this data, or as the United States terms it: "identified data," has in fact been retained by law enforcement.

- **Fifth**, as a result of the search in step three, law enforcement created a second set of data, the "remaining data," from the seized device of which it determined it was not allowed to retain possession.

    - In at least one search warrant application pursuant to Federal Rule 41, the applicant indicates that it is possible that law enforcement may discovery incriminating data that falls outside the confines of the search warrant application. In that instance law enforcement indicates it will seek an additional warrant.[2]

[2] Bates 8562 (3:24-mj-481): "Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment 8. To the extent they

  - This indicates that law enforcement is indeed scouring the "remaining data" for information that is outside the scope of the search warrant.

- **Sixth**, law enforcement has maintained possession of 1) the seized device containing all the data, 2) the "identified data", and 3) the "remaining data."

In the above process, there can be no argument, law enforcement has, in fact, seized the device, all the data, and possesses both. The United States attempts to frame the issue as whether or not It is "'authorized to seize' Remaining Data." Doc 30 at pg 5. This is obviously an incorrect framing, the warrant authorized **seizure**, the warrant authorized a **search**, the issue is whether or not the warrant authorized the government to **possess** the remaining data, which considering that the government currently maintains possession of, and seeks a protective order preventing dissemination of, the "remaining data," it is obviously that the government still possesses the data.[3]

discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant."

[3] Bates 8746 (3:25-mj-317): A search warrant application for iphones seized by law enforcement. This search warrant differs from the search warrant contained in 3:24-mj-481 (discussed *infra*: Argument, Brady and Rule 3.8(d)) as this search warrant application contains no indication of the process law enforcement will utilize.

Further, the search warrant application specifically states: "In addition, nothing in this warrant authorizes the government to retain any Electronically Stored Information that is not the subject of the warrant after any legitimate law enforcement purpose has ended with respect to Electronically Stored Information that is the subject of the warrant, except as otherwise permitted by the Federal Rules of Criminal Procedure."

ARGUMENT

Rule 16

Federal Rule of Criminal Procedure 16(d)(1) authorizes a court, upon a showing of good cause, to issue a protective order regarding discovery. A finding of "good cause" requires a specific showing of harm and cannot be based on broad, conclusory allegations. *United States v. Sikes*, No. 4:15CR3128, 2016 WL 6495500, at *2 (D. Neb. Nov. 2, 2016) (referencing *United States v. Bulger*, 283 F.R.D. 46, 52 (D. Mass. 2012))[4].

In United States v. Pelton, 578 F.2d 701, the defendant requested to inspect tape recordings in the government's possession. The United States sought a protective order and in support of the protective order made an ex parte presentation to the court where the court listened to the tapes. The court then determined that the tapes contained no exculpatory information and issued the protective order. The United States in this case makes no attempt to provide such a record for this Court, but rather simply concludes it seized, searched, divvied up, then dispossessed itself of information it continues to retain.

The burden for a protective order is on the party requesting, not on the defendant / respondent.

[4] In *Sikes*, the United States and the Defendant jointly requested a protective order preventing disclosure of federal discovery materials to a plaintiff in a state civil lawsuit. The Nebraska District Court initially rquired the parties to supplement their motion for protective order required the proposed protective order to be "narrowly tailored to the parties needs, and providing factual support for a finding of 'good cause' with respect to documents to be protected…" *Sikes*, No. 4:15CR3128, 2016 WL 6495500, at *3.

The United States correctly asserts that "[I]t bears the burden of showing that good cause exists for its issuance." *Doc 130 at pg 3. (*citing *United States v. Ladeaux*, 61 F.4th 582, 586 (8th Cir. 2023). The *Ladeaux* court, in saying that the government has the burden cites to *United States v. Dixon*, 355 F.Supp.3d 1. *Dixon*, specifically noted, first, that "Good cause requires a 'particularized, specific showing." *Id*, at 4. And second, noted that when determining if good cause exists, courts consider "whether (1) disclosure of the materials in question would pose a hazard to others; (2) the defendant would be prejudiced by a protective order; and (3) the public's interests in disclosure outweighs to possible harm." *Id*. *Dixon* also mentions courts consider "the safety of witnesses and other, a particular danger of perjury or witness intimidation, and the protection of information vital to national security*." Id*.

None of the considerations the *Dixon* court, referenced by the Eighth Circuit in *Ladeaux*, weigh in favor of a protective order in this case. In this case, the United States seeks to retain exclusive possession of data it seized, and searched, under the auspice that it is protecting the privacy of a person whose privacy it has already invaded (albeit pursuant to court order).

4th Amendment

The 4th Amendment commands that people are "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Search warrants authorize law enforcement to conduct reasonable searches and seizures.

Generally, a search warrant must establish probable cause to show evidence of a crime exists at a specific location, and state with specificity the thing to be searched.

The 4th Amendment does not protect Citizen A from an unreasonable search perpetrated by Citizen B. The 4th Amendment protects Citizen A from an unreasonable search conducted by the government. "[T]he Supreme Court has long held, this protection, [to be free from unreasonable searches and seizures,] extends only to actions undertaken by government officials or those acting at their direction. *United States v. Highbull*, 894 F.3d 988, 991 (8th Cir. 2018).

The United States has already searched all the data. The 4th Amendment does not prohibit the United States from disclosing data it possesses. The search warrants that authorized the United States to seize the data then search it make no condition that the United States shall not be subject to the obligations provided by court rules, state and federal statutes, professional ethics or anything else.

Federal Rule 41

Initially, the government alleges that Rule 41(e)(2)(B) authorized a 2-part seizure / search as discussed in its brief and below. The government fails to identify with particularity which devices, if any, were searched pursuant to Rule 41. Further, the United States fails to identify which devices at all it currently wishes to include in the protective order.

Federal Rule of Criminal Procedure 41(e)(2)(B) allows a court to authorize "**seizure** of electronic storage media or the seizure or copying of electronically stored information" with a "later review of the media or information consistent with the warrant." (emphasis added). The Committee Notes from the 2009 Amendment to Rule 41 indicates that the reason for the 2-step process noted above is because "electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all the information during the execution of the warrant at the search location." Nothing in Rule 41 purports to claim that the 2-step process provides any protection to the property owner, but rather why the search is separate from the seizure.

The 1989 Notes of Advisory Committee discusses the 1989 amendment, for the first time, recognizing the property owner's property rights and the owner's right to return of the seized property. The 2009 Committee Notes addresses the electronic property owner's possessory expectations, but only in the context of timing, not in the context of privacy. The Notes says: "It was not the intent of the amendment to leave the property owner without an expectation of the timing for the return to of the property…."

The privacy of the property owner has already yielded to law enforcement's search warrant issued by the court.

Brady and Rule 3.8(d)

The United States cites to a number of district court orders from various federal districts which purport to support Its position, but glosses over its obligations under Brady and Rule 3.8 of the North Dakota Rules of Professional Conduct. *Brady* generally requires the government to disclose exculpatory material and impeachment evidence. *See United states v. Robinson*, 809 F.3d 991, 996 (8th Cir. 2018). *Brady* extends to materials that, "whatever their other characteristics, may be used to impeach a witness." *Strickler v. Green*, 527 U.S. 263, 282, n.21 (1999). There are "three components or essential elements of a *Brady* prosecutorial misconduct claim: 'The evidence at issue must be favorable to the accused, either because it is exculpatory, or because it is impeaching; that evidence must have been suppressed by the State, either willfully or **inadvertently**; and prejudice must have ensued.'" *Banks v. Dretke*, 540 U.S. 668, 691 (2004) (quoting *Strickler*, 527 U.S. 263, 281-282) (emphasis added). *Banks* further held that "Our decisions lend no support to the notion that defendants must scavenge for hints of undisclosed *Brady* material when the prosecution represents that all such material has been disclosed." *Id*.

The United States asks this Court to issue a protective order relieving it of its *Brady* obligation to disclose impeachment information from data it has already searched and seeks to shift the burden to the defendant to identify impeachment information contained on devices the government possesses but that the defendant has had no opportunity to review. *Banks* suggests that it is a *Brady* violation if the government, in its initial search to identify material authorized by the search warrant, either willfully or inadvertently ignores impeachment material and thereafter fails to disclose it to the defendant.

Law enforcement in its application to search electronic devices specifically says it is looking for data outside the scope of the warrant. *See supra* Background, The Process, Fifth. Law enforcement isn't simply looking for responsive data. Just like when law enforcement searches a residence pursuant to a warrant, they aren't just looking for the subject matter of the warrant; they are also looking for other contraband which might be in plain view.

North Dakota Rule of Professional Responsibility 3.8(d) requires a prosecutor in a criminal case to "disclose to the defense at the earliest practical time all evidence or information known to the prosecutor that tends to negate the guilty of the accused…." The North Dakota Supreme Court has concluded that "a prosecutor's ethical obligation to disclose evidence under Rule 3.8(d) is broader than the duty under Brady or Rule 16…." *In re Disciplinary Action Against Feland*, 2012 ND 174, ¶14, 820 N.W. 672, 678.

The electronically stored data **has been** searched in its totality. The government took active steps to acquire the data. The government now seeks relief from its obligations to properly disclose data it did actively sought out.

What search criteria did the government utilize? The government does not say. What keywords were utilized? The government does not say.[5] What algorithms were utilized? The government does not say. Did the search identify any impeachment material? The government does not say. Did the search identify any inculpatory material

[5] Bates 8562: Search warrant application for two electronic devices. (3:24-mj-481). "Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant."

that might still qualify as impeachment? The government does not say. Did the search identify any other favorable material? The government does not say. How was the information not deemed responsive discarded or separated? The government does not say. One search warrant application specifically acknowledges that law enforcement might exceed the limitations contained in the search warrant by searching areas unrelated to search warrant "attachments" and may look at "all stored information" (3:24-mj-481):

> 9. Searching for the evidence described may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information; encode communications to avoid using key-words; attempt to delete information to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require law enforcement officers or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in the Attachments, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the DEA intends to use whatever data analysis techniques necessary to locate and retrieve the evidence sought.

What was done in this case, no information is provided save for broad conclusory allegations.

The United States references internet searches and browsing histories as privacy reasons to not disclose the information it possesses. This information is just as likely to form the basis of impeachment as it is to relate to privacy. The United States references location data, where a person has been, but this again is just as likely to result in

impeachment. And most importantly, the government already possesses and has searched this data.

The United States indicates that it seized the devices, searched the devices, created two data sets, but gives no details for how this was done. The defendant has no meaningful way to determine if the government has met or failed Its *Brady* obligation or Its Rule 3.8 obligation. The government has produced no record by which the court can make any determination that it is currently in compliance with its case, rule, or ethically mandated obligations, and yet it seeks a protective order alleviating it from any further efforts at complying related to the "vast quantities" of data it currently possesses and is obligated to review for reasons other than simply those delineated by the search warrants.

CONCLUSION

Mr. Gulden objects to the United States' request for protective order for the reasons stated above. Further, Mr. Gulden requests an opportunity to examine the government agents that currently maintain possession of the electronic data devices, the agents that "processed" the data, and agents that searched the electronically stored data.

Dated: July 15, 2025

/s/ *Stormy Vickers* (ND 6539)
Attorney for Mr. Gulden
808 3rd Ave S., Suite 201
Fargo, ND 58103
701-365-4884